

CONSTRUCTING PERMUTATION POLYNOMIALS OVER FINITE FIELDS

XIAOER QIN AND SHAOFANG HONG

ABSTRACT. In this paper, we construct several new permutation polynomials over finite fields. First, using the linearized polynomials, we construct permutation polynomials of the form $L_1(x) + (L_2(x) + \gamma)h(B(x))$ over \mathbf{F}_{q^m} , where $L_1(x)$, $L_2(x)$ and $B(x)$ are linearized polynomials. This extends a recent theorem of Akbary, Ghioca and Wang. Consequently, we generalize a result of Marcos by constructing permutation polynomials of the form $x^{q^i}h(\lambda_j(x))$ and $x^{q^i}h(\mu_j(x))$, where $\lambda_j(x)$ is the j -th elementary symmetric polynomial of $x, x^q, \dots, x^{q^{m-1}}$ and $\mu_j(x) = \text{Tr}_{E/K}(x^j)$. Finally, we describe the relationship between Kloosterman polynomials and permutation polynomials over finite fields with any characteristic p . It extends a result of Yuan, Ding, Wang and Pieprzyk. By our relationship, we determine some permutation polynomials of the form $(x^{2^i} + x + \eta)^{-2^j} + x^{2^k}$ over \mathbf{F}_{2^m} , where $\text{Tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}(\eta) = 1$. We also show that $(x^4 + x + \eta)^{-1} + x^2$ with $\eta \in \mathbf{F}_{2^4}$ and $\text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_2}(\eta) = 1$ is a permutation polynomial over \mathbf{F}_{2^4} .

1. Introduction

Let \mathbf{F}_q denote the finite field of characteristic p with q elements ($q = p^n, n \in \mathbf{N}$), and let $\mathbf{F}_q^* := \mathbf{F}_q \setminus \{0\}$. Let $\mathbf{F}_q[x]$ be the ring of polynomials over \mathbf{F}_q in the indeterminate x . If a polynomial $f(x) \in \mathbf{F}_q[x]$ induces a bijective map from \mathbf{F}_q to itself, then $f(x)$ is called a *permutation polynomial* of \mathbf{F}_q . Permutation polynomials have been an interesting subject of study in the area of finite fields for many years. Particularly, permutation polynomials have many important applications in coding theory [6], cryptography [11] and combinatorial design theory. Information about properties, constructions and applications of permutation polynomials may be found in the renowned book of Lidl and Niederreiter [9].

We let $K = \mathbf{F}_q$ and $E = \mathbf{F}_{q^m}$ with $m > 1$ being a given integer. By $\text{Tr}_{E/K}(x)$ we denote the *trace* from E to K , that is

$$\text{Tr}_{E/K}(x) = x + x^q + \dots + x^{q^{m-1}}.$$

A polynomial of the form

$$L(x) = \sum_{i=0}^{m-1} a_i x^{q^i} \in E[x]$$

is called a *linearized polynomial* over E . It is well known that a linearized polynomial $L(x)$ is a permutation polynomial of E if and only if the set of roots in E of $L(x)$

Date: March 13, 2013.

Key words and phrases. Permutation polynomial, Kloosterman polynomial, linearized polynomial, elementary symmetric polynomial, trace, norm.

Hong is the corresponding author and was supported partially by the Ph.D. Programs Foundation of Ministry of Education of China Grant #20100181110073.

equals $\{0\}$ (see, for example, Theorem 7.9 of [9]). Throughout, $L(x)$ denotes a linearized polynomial.

To find new classes of permutation polynomials is one of open problems raised by Lidl and Mullen in [7] and [8]. There has been significant progress in finding new permutation polynomials. Wan and Lidl [12] constructed permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and studied their group structure. Akbary, Ghioca and Wang [1] constructed permutations of the shape $L_1(x) + L_2(x)h(L_3(x))$ with $h(x)$ being a polynomial over E . Yuan, Ding, Wang and Pieprzyk [13] studied the permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$. Coulter, Henderson and Matthews [2] constructed the permutation polynomials of the form $L(x) + xh(\text{Tr}_{E/K}(x))$. Marcos [10] obtained permutation polynomials of the form $L(x) + \gamma h(\text{Tr}_{E/K}(x))$. For some other permutation polynomials constructed using the trace function, the readers are referred to [4].

The main goal of the present paper is to construct new classes of permutation polynomials over finite fields. In Section 2, we construct some permutation polynomials using linearized polynomials. In fact, we obtain a characterization so that $L_1(x) + (L_2(x) + \gamma)h(B(x)) \in E[x]$ with $L_1(x)$, $L_2(x)$ and $B(x)$ being linearized polynomials, is a permutation polynomial. See Theorem 2.1 below, which extends a recent theorem of Akbary, Ghioca and Wang [1]. Note that our method is different from that of [1]. If taking $B(x) = \text{Tr}_{E/K}(x)$, then our result (Theorem 2.2 below) generalizes the results obtained by Coulter, Henderson and Matthews [2] and by Marcos [10], respectively.

For any integer $1 \leq j \leq m-1$, let $\mu_j(x) = \text{Tr}_{E/K}(x^j)$ and $\lambda_j(x) = \sigma_j(x, x^q, \dots, x^{q^{m-1}})$, where $\sigma_j(x, x^q, \dots, x^{q^{m-1}})$ is the j -th elementary symmetric polynomial of $x, x^q, \dots, x^{q^{m-1}}$. Marcos [10] used the function $\lambda(x) (= \lambda_2(x) \text{ or } \mu_2(x))$ to construct permutation polynomials and only got some sufficient conditions so that $xh(\lambda(x))$ to be a permutation polynomial. In Section 3, using $\lambda_j(x)$ and $\mu_j(x)$, we extend this result by giving sufficient and necessary conditions so that $x^{q^i}h(\lambda_j(x))$ and $x^{q^i}h(\mu_j(x))$ to be permutation polynomials.

In 2008, Yuan et al. [13] described the relationship between Kloosterman polynomials $L_{1,d}$ and permutation polynomials of a special form, and then presented several classes of permutation polynomials related to the Kloosterman polynomial $L_{1,10}$. In Section 4, we extend this characterization by providing the relationship between Kloosterman polynomials $L_{p^i,d}(x)$ and permutation polynomials $\frac{1}{L_d(x)+\eta} + x^{p^i}$ over finite fields of any characteristic p , where $\text{Tr}_{E/K}(\eta) \neq 0$. Then using this result and Hollmann-Xiang theorem, we produce some new permutation polynomials of the form $(x^{2^i} + x + \eta)^{-2^j} + x^{2^k}$ over \mathbf{F}_{2^m} , where $\text{Tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}(\eta) = 1$, $i = 1, 2$, $0 \leq k \leq m-1$ and $j = k$ or $j = k+1$. In particular, we show that $\frac{1}{x^4+x+\eta} + x^2$ with $\eta \in \mathbf{F}_{2^4}$ and $\text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_2}(\eta) = 1$ is a permutation polynomial over \mathbf{F}_{2^4} .

2. Permutation polynomials constructed by the linearized polynomials

In this section, we construct a new class of permutation polynomials involving linearized polynomials. We need the following known facts in the sequel.

Lemma 2.1. *Let $B(x) \in K[x]$ and $L(x) \in K[x]$ be linearized polynomials. Then for any $a \in K$ and x and $y \in E$, $aB(x) = B(ax)$, $B(x+y) = B(x) + B(y)$ and $B(L(x)) = L(B(x))$.*

We can now give the first main result of this paper.

Theorem 2.1. *Let $\gamma \in E$ and let $L_1(x) \in K[x]$, $L_2(x) \in K[x]$ and $B(x) \in K[x]$ be linearized polynomials. Let $h(x) \in E[x]$ be such that $h(B(E)) \subseteq K$. Then $F(x) := L_1(x) + (L_2(x) + \gamma)h(B(x))$ is a permutation polynomial over E if and only if each of the following is true:*

- (1). $L_1(x) + (L_2(x) + B(\gamma))h(x)$ permutes $B(E)$.
- (2). For any $y \in B(E)$, $L_1(x) + L_2(x)h(y) = 0$ and $B(x) = 0$ with $x \in E$ are both true if and only if $x = 0$.

Proof. First we show the sufficiency part. Assume that (1) and (2) hold. Suppose that there exist two elements α and $\beta \in E$ such that $F(\alpha) = F(\beta)$. Thus $B(F(\alpha)) = B(F(\beta))$. That is,

$$B(L_1(\alpha) + (L_2(\alpha) + \gamma)h(B(\alpha))) = B(L_1(\beta) + (L_2(\beta) + \gamma)h(B(\beta))). \quad (2.1)$$

Then Lemma 2.1 applied to both sides of (2.1) gives us that

$$L_1(B(\alpha)) + (L_2(B(\alpha)) + B(\gamma))h(B(\alpha)) = L_1(B(\beta)) + (L_2(B(\beta)) + B(\gamma))h(B(\beta)). \quad (2.2)$$

Since $L_1(x) + (L_2(x) + B(\gamma))h(x)$ permutes $B(E)$, it follows from (2.2) that $B(\alpha) = B(\beta)$. Write $t := B(\alpha) = B(\beta)$. Then $t \in B(E)$ and $B(\alpha - \beta) = 0$. Since $F(\alpha) = F(\beta)$, one has

$$L_1(\alpha - \beta) + L_2(\alpha - \beta)h(t) = 0.$$

Now applying condition (2) to $\alpha - \beta$, we obtain that $\alpha - \beta = 0$ which implies that $\alpha = \beta$. Hence $F(x)$ is a permutation polynomial over E . The sufficiency part is proved.

Let us now show the necessity part. Let $F(x)$ be a permutation polynomial of E . First we prove that (1) is true. To do so, we let $B(x)$ act on $F(x)$ for $x \in E$, and then by Lemma 2.1 we get that

$$B(F(x)) = L_1(B(x)) + (L_2(B(x)) + B(\gamma))h(B(x)). \quad (2.3)$$

Since $F(x)$ is a permutation polynomial of E , we have

$$|\{B(F(x)) : x \in E\}| = |\{B(x) : x \in E\}| = |B(E)|. \quad (2.4)$$

Hence by (2.3) and (2.4),

$$|\{L_1(B(x)) + (L_2(B(x)) + B(\gamma))h(B(x)) : x \in E\}| = |B(E)|.$$

This concludes that $L_1(x) + (L_2(x) + B(\gamma))h(x)$ permutes $B(E)$. Thus (1) is proved.

It remains to show that part (2) is true. For this purpose, we assume that for any $y \in B(E)$, $L_1(x) + L_2(x)h(y) = 0$ and $B(x) = 0$ with $x \in E$. We can take two elements α and $\beta \in E$ satisfying that $B(\alpha) = B(\beta) = y$. Then $B(\alpha - \beta) = 0$. But $B(x) = 0$. Therefore $\alpha - \beta$ and x are both in the kernel $\ker(B)$ of $B(x)$. So we can write $x = \alpha - \beta + z$ for some $z \in \ker(B)$. Since $L_1(x) + L_2(x)h(y) = 0$, we infer that

$$L_1(\alpha - \beta + z) + L_2(\alpha - \beta + z)h(y) = 0. \quad (2.5)$$

On the other hand, since $z \in \ker(B)$, one has $B(z) = 0$, which implies that $B(\beta - z) = B(\alpha) = y$. It then follows immediately that

$$\begin{aligned} & F(\alpha) - F(\beta - z) \\ &= L_1(\alpha) + (L_2(\alpha) + \gamma)h(B(\alpha)) - L_1(\beta - z) + (L_2(\beta - z) + \gamma)h(B(\beta - z)) \\ &= L_1(\alpha - \beta + z) + L_2(\alpha - \beta + z)h(y). \end{aligned} \quad (2.6)$$

Hence by (2.5) and (2.6), we derive that $F(\alpha) = F(\beta - z)$. Since $F(x)$ is a permutation polynomial of E , we get that $\alpha - \beta + z = 0$. Namely, $x = 0$. Thus (2) is proved.

This completes the proof of Theorem 2.1. \square

Picking $\gamma = 0$, then Theorem 2.1 gives us the following result which is Theorem 6.1 of [1].

Corollary 2.1. [1] *Let L_1, L_2 and L_3 be K -linear polynomials over K . Let $h(x) \in E[x]$ and $h(L_3(E)) \subseteq K$. Then the polynomial $F(x) := L_1(x) + L_2(x)h(L_3(x))$ is a permutation polynomial over E if and only if each of the following is true:*

- (1). $L_1(x) + L_2(x)h(x)$ permutes $L_3(E)$.
- (2). For any $y \in L_3(E)$, $L_1(x) + L_2(x)h(y) = 0$ and $L_3(x) = 0$ with $x \in E$ are both true if and only if $x = 0$.

As another special case of Theorem 2.1, we have the following interesting result.

Theorem 2.2. *Let $L_1(x) \in K[x]$ and $L_2(x) \in K[x]$ be linearized polynomials. Let $h(x) \in K[x]$ and $\gamma \in E$. Then $F(x) := L_1(x) + (L_2(x) + \gamma)h(\text{Tr}_{E/K}(x))$ is a permutation polynomial over E if and only if each of the following is true:*

- (1). $L_1(x) + (L_2(x) + \text{Tr}_{E/K}(\gamma))h(x) \in K[x]$ is a permutation polynomial over K .
- (2). For any $y \in K$, $L_1(x) + L_2(x)h(y) = 0$ and $\text{Tr}_{E/K}(x) = 0$ with $x \in E$ are both true if and only if $x = 0$.

Proof. Let $B(x) = \text{Tr}_{E/K}(x)$. Then $B(x)$ is a linearized polynomial. So Theorem 2.2 follows immediately from Theorem 2.1. This completes the proof of Theorem 2.2. \square

From Theorem 2.2, we derive the following interesting consequences.

Corollary 2.2. [2] *Let $F(x) := L(x) + xh(\text{Tr}_{E/K}(x))$ with $L(x) \in K[x]$ being a linearized polynomial and $h(x) \in K[x]$. Then $F(x)$ is a permutation polynomial over E if and only if each of the following is true:*

- (1). $L(x) + xh(x)$ is a permutation polynomial over K .
- (2). For any $y \in K$, we have that $x \in E$ satisfies $L(x) + xh(y) = 0$ and $\text{Tr}_{E/K}(x) = 0$ if and only if $x = 0$.

Proof. This corollary follows from Theorem 2.2 by setting $L_1(x) = L(x)$, $L_2(x) = x$ and $\gamma = 0$. The proof of Corollary 2.2 is complete. \square

Corollary 2.3. [10] *Let $L(x) = a_0x + a_1x^q + \cdots + a_{m-1}x^{q^{m-1}} \in K[x]$ be a linearized polynomial which permutes E . Let $h(x) \in K[x]$ and $\gamma \in E$. Then the polynomial $F(x) := L(x) + \gamma h(\text{Tr}_{E/K}(x))$ permutes E if and only if the polynomial $(a_0 + a_1 + \cdots + a_{m-1})x + \text{Tr}_{E/K}(\gamma)h(x)$ permutes K .*

Proof. Since $L(x)$ is a permutation of E , we have that for any $x \in E$, $L(x) = 0$ if and only if $x = 0$. So by Theorem 2.2 we know that $F(x)$ is a permutation polynomial over E if and only if $L(x) + \text{Tr}_{E/K}(\gamma)h(x)$ is a permutation polynomial over K .

On the other hand, if $x \in K$, we have $L(x) = (a_0 + a_1 + \cdots + a_{m-1})x$. It then follows that $F(x)$ is a permutation polynomial over E if and only if $(a_0 + a_1 + \cdots + a_{m-1})x + \text{Tr}_{E/K}(\gamma)h(x)$ is a permutation polynomial over K as desired. Corollary 2.3 is proved. \square

Corollary 2.4. *Let $h(x) \in K[x]$ and $0 \leq i \leq m-1$ be an integer. Then $F(x) := x^{q^i} h(\text{Tr}_{E/K}(x))$ is a permutation polynomial over E if and only if each of the following is true:*

- (1). $xh(x)$ is a permutation polynomial over K .
- (2). For any $y \in K$, we have that $x \in E$ satisfies $x^{q^i} h(y) = 0$ and $\text{Tr}_{E/K}(x) = 0$ if and only if $x = 0$.

Proof. Note that $x^{q^i} = x$ if $x \in K$. Then letting $L_1(x) = 0, L_2(x) = x^{q^i}$ and $\gamma = 0$ in Theorem 2.2 gives us the desired result. \square

Corollary 2.5. *Let $L_1(x) \in K[x]$ and $L_2(x) \in K[x]$ be linearized polynomials and $h(x) \in K[x]$. Then $F(x) := L_1(x) + L_2(x)h(\text{Tr}_{E/K}(x))$ is a permutation polynomial over E if and only if each of the following is true:*

- (1). $L_1(x) + L_2(x)h(x)$ is a permutation polynomial over K .
- (2). For any $y \in K$, we have that $x \in E$ satisfies $L_1(x) + L_2(x)h(y) = 0$ and $\text{Tr}_{E/K}(x) = 0$ if and only if $x = 0$.

Proof. This corollary follows from Theorem 2.2 by setting $\gamma = 0$. \square

In what follows we give two examples to illustrate Corollaries 2.4 and 2.5.

Example 2.1. Let $q \equiv 0 \pmod{5}$, $K = \mathbf{F}_q$ and $E = \mathbf{F}_{q^m}$ with $m > 1$ being a integer. Let $h(x) = (x^2 - a)^2 \in K[x]$, where $a \in K$ is non-square. It is known that $xh(x) = a^2x - 2ax^3 + x^5$ is a permutation polynomial over K (see for example, Table 7.1 in Page 352 of [9]). Since a is non-square, we have that $h(y) = (y^2 - a)^2 \neq 0$ for any $y \in K$. Then $x^{q^i} h(y) = 0$ and $\text{Tr}_{E/K}(x) = 0$ if and only if $x = 0$. By Corollary 2.4,

$$x^{q^i} h(\text{Tr}_{E/K}(x)) = x^{q^i} \left(\left(\sum_{j=0}^{m-1} x^{q^j} \right)^2 - a \right)^2$$

is a permutation polynomial over E for any integer $0 \leq i \leq m-1$.

Example 2.2. Let $q = 8$, $K = \mathbf{F}_q$ and $E = \mathbf{F}_{q^m}$ with $m > 1$ being an odd integer. Let $h(x) = x^3 - ax$, $L_1(x) = a^2x$ and $L_2(x) = x^2$, where $a \in K^*$. Then $L_1(x) + L_2(x)h(x) = D_5(x, a)$, where $D_5(x, a)$ is the Dickson polynomial of degree 5 over K . Since $\gcd(5, q^2 - 1) = 1$, by Theorem 7.16 of [9] we know that $D_5(x, a)$ is a permutation polynomial over K . That is, $L_1(x) + L_2(x)h(x) = x^5 - ax^3 + a^2x$ is a permutation polynomial over K . Let $y \in K$ be any element and $x \in E$ satisfy that $\text{Tr}_{E/K}(x) = 0$ and $L_1(x) + L_2(x)h(y) = 0$. If $h(y) = 0$, then $\text{Tr}_{E/K}(x) = 0$ and $L_1(x) = 0$. From $L_1(x) = a^2x = 0$, we derive that $x = 0$. If $h(y) \neq 0$, it then follows from $L_1(x) + L_2(x)h(y) = 0$ that $x = 0$ or $x = \frac{a^2}{y^3 - ay} \neq 0$. Assume that $x = \frac{a^2}{y^3 - ay}$. Then

$$\text{Tr}_{E/K}(x) = \text{Tr}_{E/K}\left(\frac{a^2}{y^3 - ay}\right) = \frac{ma^2}{y^3 - ay} \neq 0$$

since m is odd and $\frac{a^2}{y^3 - ay} \neq 0$. Thus we conclude that for any $y \in K$, $\text{Tr}_{E/K}(x) = 0$ and $L_1(x) + L_2(x)h(y) = 0$ if and only if $x = 0$. Now by Corollary 2.5, we get that

$$L_1(x) + L_2(x)h(\text{Tr}_{E/K}(x)) = a^2x + x^2(\text{Tr}_{E/K}(x)^3 - a\text{Tr}_{E/K}(x))$$

is a permutation polynomial over E .

3. Permutation polynomials constructed by the elementary symmetric polynomials

Throughout this section, let m and j be positive integers such that $1 \leq j \leq m-1$. Let $\sigma_j(x_1, \dots, x_m)$ denote the j -th elementary symmetric polynomial in m variables x_1, \dots, x_m . That is, one has

$$\sigma_j(x_1, \dots, x_m) = \sum_{1 \leq i_1 < \dots < i_j \leq m} x_{i_1} \dots x_{i_j}.$$

Then we can define the polynomial $\lambda_j(x)$ by

$$\lambda_j(x) := \sigma_j(x, x^q, \dots, x^{q^{m-1}}) = \sum_{0 \leq i_1 < i_2 < \dots < i_j \leq m-1} x^{q^{i_1} + \dots + q^{i_j}}.$$

Marcos [10] used the polynomials $\lambda_2(x)$ and $\text{Tr}_{E/K}(x^2)$ to give two sufficient conditions such that $xh(\lambda_2(x))$ and $xh(\text{Tr}_{E/K}(x^2))$ are permutation polynomials.

In this section, we construct two new classes of permutation polynomials by using the functions $\lambda_j(x)$ and $\text{Tr}_{E/K}(x^j)$. We begin with the following two lemmas which will be needed in the sequel.

Lemma 3.1. *Let $\alpha \in E$ and $a \in K$. Then $\lambda_j(x) \in K[x]$, $\lambda_j(\alpha) \in K$, $\lambda_j(\alpha^q) = \lambda_j(\alpha)$ and $\lambda_j(a\alpha) = a^j \lambda_j(\alpha)$.*

Proof. By the definition of λ_j , one can easily check that Lemma 3.1 is true. \square

Lemma 3.2. *For any integer j satisfying that $1 \leq j \leq m-1$ and $\gcd(j, q-1) = 1$, $\lambda_j(x)$ is a mapping from E onto K .*

Proof. First we show that there is an $\alpha \in E$ such that $\lambda_j(\alpha) \neq 0$. Since $\lambda_j(x)$ has at most

$$\deg(\lambda_j(x)) = q^{m-j} + \dots + q^{m-1} \leq q + \dots + q^{m-1} = \frac{q^m - 1}{q - 1} - 1 < q^m = |E|$$

roots in E , there exists an element $\alpha \in E$ such that $\lambda_j(\alpha) \neq 0$. Now pick an $\alpha \in E$ such that $a := \lambda_j(\alpha) \neq 0$. In what follows, we show that for any $b \in K$, we can find an element $\beta \in E$ such that $\lambda_j(\beta) = b$.

Since $\gcd(j, q-1) = 1$, by Theorem 7.8 of [9] we know that ax^j is a permutation polynomial over K . It follows that for any given $b \in K$, there exists an element $c \in K$ such that $b = ac^j$. Since $\lambda_j(\alpha) = a$, letting $\beta := c\alpha$ gives us that

$$\lambda_j(\beta) = \lambda_j(c\alpha) = c^j \lambda_j(\alpha) = ac^j = b$$

as desired. Thus Lemma 3.2 is proved. \square

Using the polynomials $\lambda_j(x)$, we can give the following characterization on permutation polynomials of the form $x^{q^i} h(\lambda_j(x))$.

Theorem 3.1. *Let m, i and j be positive integers such that $0 \leq i \leq m-1$ and $1 \leq j \leq m-1$ and $\gcd(j, q-1) = 1$. Let $h(x) \in K[x]$. Then $x^{q^i} h(\lambda_j(x))$ is a permutation polynomial over E if and only if $h(0) \neq 0$ and $xh(x)^j$ permutes K .*

Proof. Write $F(x) := x^{q^i} h(\lambda_j(x))$. First we show the sufficiency part. Since $xh(x)^j$ permutes K , we obtain that $xh(\delta)^j \neq 0$ for $\delta \in K^*$. We get that $h(\delta) \neq 0$ for $\delta \in K^*$. But $h(0) \neq 0$. Hence $h(\delta) \neq 0$ for all $\delta \in K$.

Now we choose two elements $\alpha, \beta \in E$ such that $F(\alpha) = F(\beta)$, namely

$$\alpha^{q^i} h(\lambda_j(\alpha)) = \beta^{q^i} h(\lambda_j(\beta)). \quad (3.1)$$

Then $\lambda_j(F(\alpha)) = \lambda_j(F(\beta))$. Using Lemma 3.1, we infer that

$$\lambda_j(\alpha) h(\lambda_j(\alpha))^j = \lambda_j(\beta) h(\lambda_j(\beta))^j. \quad (3.2)$$

Since $xh(x)^j$ permutes K , (3.2) tells us that $\lambda_j(\alpha) = \lambda_j(\beta)$. It then follows from (3.1) that $\alpha^{q^i} = \beta^{q^i}$. Thus $\alpha = \beta$ since x^{q^i} is a permutation polynomial over E . Hence $F(x)$ is a permutation polynomial over E . The sufficiency part is proved.

Let us now show the necessity part. Assume that $F(x)$ is a permutation polynomial over E . First we prove that $h(0) \neq 0$. By Lemma 3.2, we know that $\lambda_j(x)$ is a mapping from E onto K if $\gcd(j, q-1) = 1$. For $1 \leq j \leq m-1$, one has that

$$\deg \lambda_j(x) = q^{m-j} + \dots + q^{m-1} \leq q + \dots + q^{m-1}.$$

Thus for any $a \in K^*$, the equation $\lambda_j(x) = a$ has at most $q + \dots + q^{m-1}$ roots in E . Then the equation $\lambda_j(x) = 0$ has at least $q^m - (q-1)(q + \dots + q^{m-1}) = q$ roots in E . Hence $\lambda_j(x) = 0$ has a nonzero root in E . We pick $\alpha \in E^*$ such that $\lambda_j(\alpha) = 0$. Then $\alpha^{q^i} h(0) = \alpha^{q^i} h(\lambda_j(\alpha)) = F(\alpha)$. Since $F(x)$ is a permutation polynomial over E and α is nonzero, we have $F(\alpha) \neq 0$. That is, $\alpha^{q^i} h(0) \neq 0$. Thus $h(0) \neq 0$.

It remains to show that $xh(x)^j$ permutes K . On the one hand, by Lemma 3.1 we have

$$\lambda_j(F(x)) = \lambda_j(x) h(\lambda_j(x))^j. \quad (3.3)$$

On the other hand, by Lemma 3.2 we know that for all integer j with $1 \leq j \leq m-1$ and $\gcd(j, q-1) = 1$, $\lambda_j(x)$ is a mapping from E onto K . This implies that

$$\{xh(x)^j : x \in K\} = \{\lambda_j(x) h(\lambda_j(x))^j : x \in E\}. \quad (3.4)$$

Since $F(x)$ permutes E , it then follows from (3.3) and (3.4) that

$$\begin{aligned} |\{xh(x)^j : x \in K\}| &= |\{\lambda_j(x) h(\lambda_j(x))^j : x \in E\}| = |\{\lambda_j(F(x)) : x \in E\}| \\ &= |\{\lambda_j(x) : x \in E\}| = q. \end{aligned}$$

Hence $xh(x)^j$ permutes K . The necessity part is proved.

The proof of Theorem 3.1 is complete. \square

Now define $\mu_j(x) := \sum_{i=0}^{m-1} x^{jq^i} = \text{Tr}_{E/K}(x^j)$ for $1 \leq j \leq q^m - 1$. Then $\mu_j(x) \in K[x]$, $\mu_j(\alpha) \in K$ and $\mu_j(a\alpha) = a^j \mu_j(\alpha)$ for all $a \in K$ and $\alpha \in E$. Also $\mu_j(x)$ is a mapping from E onto K if $\gcd(j, q^m - 1) = 1$. Replaced $\lambda_j(x)$ by $\mu_j(x)$, we can characterize the permutation polynomials of the form $x^{q^i} h(\mu_j(x))$ as follows. The proof of Theorem 3.2 is similar as that of Theorem 3.1 and so we just give a sketch of the proof.

Theorem 3.2. *Let m, i and j be positive integers such that $0 \leq i \leq m-1$ and $1 \leq j \leq q^m - 1$ and $\gcd(j, q^m - 1) = 1$. Let $h(x) \in K[x]$. Then $x^{q^i} h(\mu_j(x))$ is a permutation polynomial over E if and only if $h(0) \neq 0$ and $xh(x)^j$ permutes K .*

Proof. We here merely prove that if $x^{q^i} h(\mu_j(x))$ is a permutation polynomial over E , then $h(0) \neq 0$. The other part of the proof is similar to that of Theorem 3.1.

Assume that $x^{q^i} h(\mu_j(x))$ is a permutation polynomial over E . Clearly, there exists a nonzero element θ such that $\text{Tr}_{E/K}(\theta) = 0$. Since $\gcd(j, q^m - 1) = 1$, x^j permutes E . So there is a nonzero element $\omega \in E$ such that $\omega^j = \theta$. Therefore $\text{Tr}_{E/K}(\omega^j) = 0$, i.e.,

$\mu_j(\omega) = 0$. Then $\omega^{q^i} h(0) = \omega^{q^i} h(\mu_j(\omega))$. Since $x^{q^i} h(\mu_j(x))$ is a permutation polynomial over E and ω is nonzero, we have $\omega^{q^i} h(0) \neq 0$. Thus $h(0) \neq 0$.

This completes the proof of Theorem 3.2. \square

Picking $j = 2$, then the sufficiency part of Theorems 3.1 and 3.2 becomes Proposition 12 of [10].

4. Permutation polynomials constructed by Kloosterman polynomials

In this section, let p be a prime and denote $K = \mathbf{F}_p$ and $E = \mathbf{F}_{p^m}$ with $m > 1$ being an integer. For any $e \in K$, define $T_e := \{x \in E \mid \text{Tr}_{E/K}(x) = e\}$. Let c be an integer in $\{1, 2, \dots, p^m - 1\}$ and the p -adic representation of c be $c = \sum_{i=0}^{m-1} c_i p^i$ with $c_i \in \{0, 1, \dots, p-1\}$. Then the *weight* $w(c)$ of c is defined by $w(c) := \sum_{i=0}^{m-1} c_i$. Define the polynomial L_c on E as

$$L_c(x) := \sum_{i=0}^{m-1} c_i x^{p^i}.$$

For integers $c, d \in \{1, 2, \dots, p^m - 1\}$, we define the polynomial $L_{c,d}$ on E as

$$L_{c,d}(x) := L_c(x) + L_d(x^{p^m-2}).$$

Then we can rewrite $L_{c,d}$ as

$$L_{c,d}(x) = L_c(x) + L_d\left(\frac{1}{x}\right)$$

with the convention that $L_{c,d}(0) := 0$.

Following [3], we call $L_{c,d}(x)$ a *Kloosterman polynomial* on E if the function $L_{c,d}$ induced by $L_{c,d}(x)$ is a bijection from T_i to $T_{i'}$ for all $i = 1, 2, \dots, p-1$, where i' depends on i and $L_{c,d}(x)$. We can now extend the Yuan-Ding-Wang-Pieprzyk theorem [13] as follows.

Theorem 4.1. *Let i and d be integers such that $0 \leq i \leq m-1$ and $d \in \{1, 2, \dots, p^m - 1\}$ with $w(d) \equiv 0 \pmod{p}$. Then $L_{p^i,d}(x)$ is a Kloosterman polynomial on E if and only if for any $\eta \in E$ with $\text{Tr}_{E/K}(\eta) \neq 0$, $\frac{1}{L_d(x) + \eta} + x^{p^i}$ is a permutation polynomial over E .*

Proof. Write $d := \sum_{i=0}^{m-1} d_i p^i$. Then $L_d(x) := \sum_{i=0}^{m-1} d_i x^{p^i}$ with $d_i \in \{0, 1, \dots, p-1\}$. Hence $\text{Tr}_{E/K}(L_d(x)) = w(d)\text{Tr}_{E/K}(x)$ for any $x \in E$. In fact, one has

$$\text{Tr}_{E/K}(L_{p^i,d}(x)) = \text{Tr}_{E/K}(x^{p^i} + L_d\left(\frac{1}{x}\right)) = \text{Tr}_{E/K}(x) + w(d)\text{Tr}_{E/K}\left(\frac{1}{x}\right).$$

Clearly, for $w(d) \equiv 0 \pmod{p}$, we have $\text{Tr}_{E/K}(L_{p^i,d}(x)) = \text{Tr}_{E/K}(x)$.

First we show the sufficiency part. Assume that $L_{p^i,d}(x)$ is a Kloosterman polynomial on E . Since $w(d) \equiv 0 \pmod{p}$, for any $x \in T_l$ with $l \in \{0, 1, 2, \dots, p-1\}$, we have $\text{Tr}_{E/K}(L_{p^i,d}(x)) = l$. Let $\eta \in E$ be such that $\text{Tr}_{E/K}(\eta) = j \neq 0$ and let $a \in E$ be an arbitrary given element. We consider the equation

$$\frac{1}{L_d(x) + \eta} + x^{p^i} = a. \quad (4.1)$$

Since x^{p^i} is permutation polynomial over E , it follows that for any $a \in E$, there exists a unique $\alpha \in E$ such that $\alpha^{p^i} = a$. It then follows from $\eta \in T_j$ and $w(d) \equiv 0 \pmod{p}$ that for any $x \in E$, we have

$$\text{Tr}_{E/K}(L_d(x) + \eta) = \text{Tr}_{E/K}(\eta) = j.$$

Thus $L_d(x) + \eta \in T_j$, which implies that $L_d(x) + \eta \neq 0$ for any $x \in E$. Therefore α cannot be a solution of (4.1).

Evidently, (4.1) is equivalent to

$$(x^{p^i} - a)(L_d(x) + \eta) + 1 = 0. \quad (4.2)$$

Since $a = \alpha^{p^i}$, (4.2) is equivalent to

$$(x - \alpha)^{p^i}(L_d(x) + \eta) + 1 = 0. \quad (4.3)$$

Let $y = x - \alpha$. Then (4.3) is equivalent to

$$y^{p^i}(L_d(y) + L_d(\alpha) + \eta) + 1 = 0. \quad (4.4)$$

Clearly $y = 0$ is not a solution of (4.4). So (4.4) is equivalent to

$$\frac{1}{y^{p^i}} + L_d(y) = -L_d(\alpha) - \eta. \quad (4.5)$$

But

$$L_{p^i,d}\left(\frac{1}{y}\right) = \frac{1}{y^{p^i}} + L_d(y).$$

Hence (4.5) is equivalent to

$$L_{p^i,d}\left(\frac{1}{y}\right) = -L_d(\alpha) - \eta. \quad (4.6)$$

Since $L_{p^i,d}(x)$ is a Kloosterman polynomial of E and $w(d) \equiv 0 \pmod{p}$, we know that $L_{p^i,d}$ maps T_l bijectively onto T_l , for $l \in \{1, 2, \dots, p-1\}$. Note that $-L_d(\alpha) - \eta \in T_{p-j}$. Thus there exists a unique element $u \in T_{p-j}$ such that $L_{p^i,d}(u) = -L_d(\alpha) - \eta$. Then $y = \frac{1}{u}$ is a unique solution of (4.6). It then follows from $y = x - \alpha$ and α being uniquely determined by a that (4.1) has a unique root x in E . Hence $\frac{1}{L_d(x)+\eta} + x^{p^i}$ is a permutation polynomial over E . The sufficiency part is proved.

Let us show the necessity part. Assume that $\eta \in T_j, j \neq 0$ and $\frac{1}{L_d(x)+\eta} + x^{p^i}$ is a permutation polynomial over E . For any $y \in T_l$ with $l \in \{1, 2, \dots, p-1\}$, we have $\text{Tr}_{E/K}(y) = l$. Since $w(d) \equiv 0 \pmod{p}$, $\text{Tr}_{E/K}(L_{p^i,d}(y)) = l$. Namely, $L_{p^i,d}(y) \in T_l$ for $l \neq 0$. It follows that for $l \neq 0$, $L_{p^i,d}(T_l) \subseteq T_l$.

Now let $b \in T_j$ with $j \in \{1, 2, \dots, p-1\}$. Then $\frac{1}{L_d(x)+b} + x^{p^i}$ is a permutation polynomial over E . It follows that there exists a unique root z in E such that

$$\frac{1}{L_d(z)+b} + z^{p^i} = 0.$$

Equivalently, there exists a unique root z in E such that $\frac{1}{z^{p^i}} + L_d(z) = -b$. In other words, there exists a unique root z in E such that $L_{p^i,d}\left(\frac{1}{z}\right) = -b$. Since $b \in T_j, -b \in T_{p-j}$. But $w(d) \equiv 0 \pmod{p}$. So we get that

$$\text{Tr}_{E/K}(-b) = \text{Tr}_{E/K}\left(L_{p^i,d}\left(\frac{1}{z}\right)\right) = \text{Tr}_{E/K}\left(\frac{1}{z}\right).$$

Hence $\text{Tr}_{E/K}\left(\frac{1}{z}\right) = p - j$. This infers that $\frac{1}{z} \in T_{p-j}$. Thus $L_{p^i,d}$ maps T_l bijectively onto T_l for $l \in \{1, 2, \dots, p-1\}$. That is, $L_{p^i,d}(x)$ is a Kloosterman polynomial of E . The necessity part is proved.

The proof of Theorem 4.1 is complete. \square

Hollmann and Xiang [5] proved the following result.

Lemma 4.1. [5] $L_{1,0}(x) = x, L_{1,3}(x) = x + \frac{1}{x} + \frac{1}{x^2}, L_{1,6}(x) = x + \frac{1}{x^2} + \frac{1}{x^4}$ and $L_{1,10}(x) = x + \frac{1}{x^2} + \frac{1}{x^8}$ are Kloosterman polynomials on \mathbf{F}_{2^m} .

Meanwhile, they also conjectured that $L_{1,d}$ is a Kloosterman polynomial on \mathbf{F}_{2^m} if and only if $d \in \{0, 3, 6, 10\}$. Further, they proved the following result.

Lemma 4.2. [5] Let $m > 1$, c and d be integers such that $c, d \in \{1, 2, \dots, 2^m - 1\}$ with $w(d)$ being even. If $L_{c,d}(x)$ is a Kloosterman polynomial on \mathbf{F}_{2^m} , then for each integer i with $0 \leq i \leq m - 1$, $L_{c,d}^{2^i}(x)$ is a Kloosterman polynomial on \mathbf{F}_{2^m} .

In [13], Yuan et al. proved that $\frac{1}{(x^4+x+\eta)^2} + x$ is a permutation polynomial over \mathbf{F}_{2^m} for any $\eta \in \mathbf{F}_{2^m}$ with $\text{Tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}(\eta) = 1$. We here use Theorem 4.1 to give the following more general results.

Theorem 4.2. Let $\eta \in \mathbf{F}_{2^m}$ with $\text{Tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}(\eta) = 1$ and i be an integer such that $0 \leq i \leq m - 1$. Then

$$\frac{1}{(x^2 + x + \eta)^{2^i}} + x^{2^i}, \frac{1}{(x^2 + x + \eta)^{2^{i+1}}} + x^{2^i}$$

and

$$\frac{1}{(x^4 + x + \eta)^{2^{i+1}}} + x^{2^i}$$

are permutation polynomials over \mathbf{F}_{2^m} .

Proof. Let i be any given integer such that $0 \leq i \leq m - 1$. Since $\text{Tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}(x) = \text{Tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}(x^{2^j})$ for any integer j with $0 \leq j \leq m - 1$, it follows that for any $\eta \in T_1$, we have that $\eta_1 := \eta^{2^i} \in T_1$ and $\eta_2 := \eta^{2^{i+1}} \in T_1$. One can easily check that $L_c^2(x) = L_{2c}(x)$. So $L_c^{2^i}(x) = L_{2^i c}(x)$. Thus we have

$$\begin{aligned} \frac{1}{(x^2 + x + \eta)^{2^i}} + x^{2^i} &= \frac{1}{L_3^{2^i}(x) + \eta_1} + x^{2^i} = \frac{1}{L_{2^i 3}(x) + \eta_1} + x^{2^i}, \\ \frac{1}{(x^2 + x + \eta)^{2^{i+1}}} + x^{2^i} &= \frac{1}{L_3^{2^{i+1}}(x) + \eta_2} + x^{2^i} = \frac{1}{L_{2^i 6}(x) + \eta_2} + x^{2^i} \end{aligned}$$

and

$$\frac{1}{(x^4 + x + \eta)^{2^{i+1}}} + x^{2^i} = \frac{1}{L_5^{2^{i+1}}(x) + \eta_2} + x^{2^i} = \frac{1}{L_{2^i 10}(x) + \eta_2} + x^{2^i}.$$

Since $L_c^{2^i}(x) = L_{2^i c}(x)$, it follows that $L_{c,d}^{2^i}(x) = L_{2^i c, 2^i d}(x)$. In particular, we have $L_{1,d}^{2^i}(x) = L_{2^i, 2^i d}(x)$ for any $d \in \{3, 6, 10\}$. By Lemmas 4.1 and 4.2, we obtain that $L_{2^i, 2^i d}(x)$ with $d \in \{3, 6, 10\}$ is a Kloosterman polynomial on \mathbf{F}_{2^m} . Then using Theorem 4.1, we know that

$$\frac{1}{L_{2^i 3}(x) + \eta_1} + x^{2^i}, \frac{1}{L_{2^i 6}(x) + \eta_2} + x^{2^i} \text{ and } \frac{1}{L_{2^i 10}(x) + \eta_2} + x^{2^i}$$

are permutation polynomials over \mathbf{F}_{2^m} . The desired results then follow immediately.

This completes the proof of Theorem 4.2. \square

Lemma 4.3. $L_{2,5}(x) = x^2 + \frac{1}{x} + \frac{1}{x^4}$ is a Kloosterman polynomial on \mathbf{F}_{2^4} .

Proof. First we can easily check that $\text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_2}(L_{2,5}(x)) = 1$ for any $x \in T_1$. Thus $L_{2,5}(T_1) \subseteq T_1$.

Now for any given $a \in \mathbf{F}_{2^4}^*$ with $\text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_2}(a) = 1$, we consider the equation $L_{2,5}(x) = a$. That is, we need to show that the following equation

$$x^2 + \frac{1}{x} + \frac{1}{x^4} = a \quad (4.7)$$

has the unique solution x . One can easily check that $x_0 := a^{11} + a^2 + a^{-1}$ is a solution of (4.7). Suppose that $x \in \mathbf{F}_{2^4}^*$ is any solution of (4.7). In what follows we show that $x = x_0$. Then

$$ax^{-4} = (x^{-2} + x^{-8}) + x^{-5} = \text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_{2^2}}(x^{-2}) + \text{N}_{\mathbf{F}_{2^4}/\mathbf{F}_{2^2}}(x^{-1}).$$

Since $\text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_{2^2}}(x^{-2}) + \text{N}_{\mathbf{F}_{2^4}/\mathbf{F}_{2^2}}(x^{-1}) \in \mathbf{F}_{2^2}$, where $a \in \mathbf{F}_{2^4}^*$ and $x \in \mathbf{F}_{2^4}^*$, it then follows that $ax^{-4} \in \mathbf{F}_{2^2}^*$.

Put $t := a^{-4}x$. Since $a^{-4}x = (ax^{-4})^{-4}$ and $a \in \mathbf{F}_{2^4}^*$ and $x \in \mathbf{F}_{2^4}^*$, we have $t \in \mathbf{F}_{2^2}^*$. With x replaced by a^4t in (4.7), we get that

$$t^2a^8 + t^{-1}a^{-4} + t^{-4}a^{-16} = a. \quad (4.8)$$

Since $t \in \mathbf{F}_{2^2}^*$, (4.8) is equivalent to

$$t^{-1}(a^8 + a^{-4} + a^{-1}) = a.$$

Thus $t = a^7 + a^{-2} + a^{-5}$. It then follows that $x = a^4t = a^{11} + a^2 + a^{-1} = x_0$ as desired. So the uniqueness of solution of (4.7) is proved. On the other hand, since $\text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_2}(a) = 1$ and $a \in \mathbf{F}_{2^4}^*$, we deduce that

$$\begin{aligned} \text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_2}(x) &= \text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_2}(a^{11} + a^2 + a^{-1}) = \text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_2}(a^{-4} + a^2 + a^{-1}) \\ &= 2\text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_2}(a^{-1}) + \text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_2}(a^2) = \text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_2}(a) = 1. \end{aligned}$$

Therefore $L_{2,5}$ maps T_1 bijectively onto T_1 . This concludes that $L_{2,5}(x)$ is a Kloosterman polynomial on \mathbf{F}_{2^4} .

The proof of Lemma 4.3 is complete. \square

Theorem 4.3. *For any $\eta \in \mathbf{F}_{2^4}$ with $\text{Tr}_{\mathbf{F}_{2^4}/\mathbf{F}_2}(\eta) = 1$, $\frac{1}{L_5(x)+\eta} + x^2 = \frac{1}{x^4+x+\eta} + x^2$ is a permutation polynomial over \mathbf{F}_{2^4} .*

Proof. Picking $p = c = 2$ and $d = 5$ in Theorem 4.1, then Theorem 4.3 follows immediately from Theorem 4.1 and Lemma 4.3. So Theorem 4.3 is proved. \square

Lemma 4.4. [3] *Let m be a positive integer. Then $L_{1,5}(x) = x - x^{3^m-2} + x^{3(3^m-2)}$ is a Kloosterman polynomial on \mathbf{F}_{3^m} .*

Using Theorem 4.1 and Lemma 4.4, we can derive the following result given in [13] as the conclusion of this paper.

Corollary 4.1. [13] *Let m be a positive integer. Then for any $\eta \in \mathbf{F}_{3^m}$ with $\text{Tr}_{E/K}(\eta) \neq 0$, $\frac{1}{L_5(x)+\eta} + x = \frac{1}{x^3-x+\eta} + x$ is a permutation polynomial over \mathbf{F}_{3^m} .*

REFERENCES

- [1] A. Akbary, D. Ghioca and Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.* 17 (2011), 51-67.
- [2] R. Coulter, M. Henderson and R. Matthews, A note on constructing permutation polynomials, *Finite Fields Appl.* 15 (2009), 553-557.
- [3] X. Cao, H.D.L. Hollmann and Q. Xiang, New Kloosterman sum identities and equalities over finite fields, *Finite Fields Appl.* 14 (2008), 823-833.
- [4] P. Charpin and G. Kyureghyan, When does $F(x) + \gamma \text{Tr}(H(x))$ permute F_{p^n} ?, *Finite Fields Appl.* 15(5) (2009), 615-632.
- [5] H.D.L. Hollmann and Q. Xiang, Kloosterman sum identities over F_{2^m} , *Discrete Math* 279 (2004), 277-286.
- [6] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, *Finite Fields Appl.* 13 (2007), 58-70.
- [7] R. Lidl and G.L. Mullen, When does a polynomial over a finite field permute the elements of the field? *Amer. Math. Monthly* 95 (1988), 243-246.
- [8] R. Lidl and G.L. Mullen, When does a polynomial over a finite field permute the elements of the field? II, *Amer. Math. Monthly* 100 (1993), 71-74.
- [9] R. Lidl and H. Niederreiter, *Finite fields, Encyclopedia of Mathematics and its Applications*, Second Ed., vol.20, Cambridge University Press, Cambridge, 1997.
- [10] J.E. Marcos, Specific permutation polynomials over finite fields, *Finite Fields Appl.* 17 (2011), 105-112.
- [11] J. Schwenk and K. Huber, Public key encryption and digital signatures based on permutation polynomials, *Electron. Lett.* 34 (1998), 759-760.
- [12] D. Wan and R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, *Monatsh. Math.* 112 (1991), 149-163.
- [13] J. Yuan, C. Ding, H. Wang and J. Pieprzyk, Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$, *Finite Fields Appl.* 14 (2008), 482-493.

MATHEMATICAL COLLEGE, SICHUAN UNIVERSITY, CHENGDU 610064, P.R. CHINA
E-mail address: qincn328@sina.com

YANGTZE CENTER OF MATHEMATICS, SICHUAN UNIVERSITY, CHENGDU 610064, P.R. CHINA AND
 MATHEMATICAL COLLEGE, SICHUAN UNIVERSITY, CHENGDU 610064, P.R. CHINA
E-mail address: sfhong@scu.edu.cn, s-f.hong@tom.com, hongsf02@yahoo.com